DOIM BULLETIN

FORT HOOD DIRECTORATE OF INFORMATION MANAGEMENT
BULLETIN No. 04-04 1114th SIGNAL BATTALION 15 MARCH 2004

Unauthorized Equipment To Be Disabled

All network devices (i.e. hubs, switches, and routers) connected to the Fort Hood ILAN must be installed and managed by DOIM authorized personnel only. Due to increasing security requirements, unauthorized user-installed devices found connected to the Fort Hood ILAN will be disabled immediately upon discovery. Once unauthorized equipment is found, the port on your hub or switch will be disabled. If you have questions about whether a device is authorized, or don't have enough LAN drops in your area, contact your IASO or G6 first and ask them to request for additional ILAN drops or to verify if the device is allowed. Be proactive and don't allow unauthorized equipment on the network. For more information, contact the networking team at the DOIM at 287-1840.

Microsoft XP Pro Now Authorized

The DOIM has issued standard software and hardware configuration guidance that says that the Microsoft XP Professional operating systems is now authorized for use on the Fort Hood ILAN. For more information, contact the DOIM Help Desk at 287-DOIM.

End of the Day Computer Procedures

The Fort Hood DOIM would like to remind all computer users that to maintain good computer operational security (OPSEC), you must take the following actions at the end of the day:

1. Log off your computer

2. Shut down your computer

3. Disconnect you network cable

With your help, we can ensure that hackers will not gain access to sensitive information. For more information, contact the DOIM Help Desk at 287-DOIM.

Disciplinary Action For Not Complying With IA Policy

Did you know that in accordance with AR 25-2, *Information Assurance*, dated 14 November 2003, Chapter 1, paragraph 1-1 (j); all personnel under the jurisdiction of UCMJ, as well as those not under UCMJ, are subject to disciplinary actions for violations of certain portions of this regulation? Check out AR 25-2 or contact your Information Assurance Security Officer (IASO) for further information.

IA Personnel Structure

The ***Information Assurance (IA) Personnel Structure*** on Fort Hood is as follows:

1. Information Assurance Manager (IAM)

2. Information Assurance Network Manager (IANM)

3. Information Assurance Security Officer (IASO)

The ***IA Support Personnel Structure*** is listed below. These people are mostly found at the unit level.

1. Systems Administrator

2. Network Administrator

3. Data Owners

4. General Users

See AR 25-2, Chapter 3, for further details or contact the Fort Hood IA Team at 287-8462 or 287-2679.

Next Active Directory Meeting – 17 March 2004

The next meeting for the Active Directory working group will be held on Wednesday, 17 March 2004, from 1130-1300 at the Fort Hood Officer's Club in the Starlight Room. For more information, contact the DOIM Systems Section at 288-0900.

DOIM BULLETIN No. 04-04

Fort Hood Directorate of Information Management
1114th Signal Battalion

Attention IASOs: New Version of the Netsky Virus

A new version of the dangerous w32_NETSKY Virus has been identified. The virus spreads through e-mail and sends itself to addresses found on the victim's machine. The virus also attempts to deactivate the w32/Mydoom.a@MM and w32/Mydoom.b@MM viruses. The virus will be received in an e-mail message that looks like this:

From: (Forged address taken from infected system)
Subject: Re: (some generic greeting or title, such as Hello, Document, Your music, Your document, Thanks!, Hi, Here, etc.)

The body of the message will tell you to look at an attached file. The attachment will most likely have a **.pif** extension, such as your_text.pif. Please make sure all your Norton Anti-Virus definitions are up-to-date and remind your personnel not to open any suspicious attachments. For more information, contact the Fort Hood IA Team at 287-8462 or 287-2679.

New Computer Naming Convention

Fort Hood is implementing a new computer naming standard to align with Army standards for naming all computer objects and to prepare for the implementation of Microsoft's Active Directory in late 2004. Computer systems and other network device names will be limited to 15 characters. The naming standard will be as follows:

1. Space 1-4 will be HOOD

2. Space 5-6 will be the Primary Function Code. This signifies what type of device it is. Examples include "WK" for workstation, "NB" for notebook, "PR" for Printer, and "DG" for Digital Sender.

3. Space 7-12 will be the Organization/Unit and Sub-organization/unit codes. This specifies what unit the device belongs to. Some examples include "DOIMOP" for Directorate of Information Management Operations Division and "4ID367" for 3-67th Armor, 4th Infantry Division.

4. Space 13-15 will be the indicator of object for uniqueness. This will be a three-digit number identifying what workstation, notebook, etc., that device is within your organization.

An example of a complete computer name is:

New Computer Naming Convention (continued)

HOODWKDOIMOP030 (the 30th desktop in the DOIM Operations Division).

For more information and a complete listing of primary function and Organization/ Unit codes, please contact the DOIM Help Desk.

Contact Information

Director: LTC Edward J. Morris Jr., 287-7109

Acting Deputy Director: Mr. Roy Walton, 287-7109

Operations Officer / S-3: MAJ Mark Dickson, 287-7289

Operations / Automations Officer: Ms. Philipa Pinkard, 287-3238

ILAN Chief (Network / Helpdesk Sections): Mr. Jimmie Moore, 287-5301

Systems Chief (LLC / NETAPPS Sections): Ms. Barbara Duckens, 287-1052

Information Assurance Branch: Mr. Jerry Brown, 287-4831, Michele Berry (IAM), 287-3261

COMMS Branch: Mr. Gary Parker, 287-5600

Plans Branch: Mr. John McFarlin, 287-7495

Services Branch: Ms. Joan Ward, 287-0040